EXHIBIT D

Brookwood

PRIVILEGED AND CONFIDENTIAL

MEMORANDUM

TO: Haseeb Qureshi, Bo Feng ("**Dragonfly**")

FROM: Collins Belton, Brookwood P.C. ("**Brookwood**")

DATE: August 24, 2020

RE: Tornado Cash Money Service Business and Money Transmitter Regulatory Analysis (the "**Analysis**")

I. Executive Summary

You have requested an analysis of regulatory considerations pertaining to Tornado Cash, an anonymizing software tool developed by PepperSec Inc. ("**PepperSec**"), in connection with a potential investment into PepperSec. Specifically, this Analysis considers the potential applicability of federal money service business regulations and state money transmission laws to PepperSec as the creator of anonymizing software for virtual currency transactions in the form of a decentralized application ("**dapp**") and as the host and operator of a front-end user interface located at tornado.cash (the "**Site**") that provides public access to the dapp's smart contracts. The scope of this Analysis is limited to an analysis under the federal Bank Secrecy Act ("**BSA**") and the regulations promulgated thereunder (the "**BSA Regulations**") in addition to an overview of potentially applicable state money transmission laws.[1] Further, this Analysis is limited to publicly available facts regarding the dapp and Site, which facts include materials referenced herein, previous written correspondence, and any other relevant prior discussions with Brookwood.

As explored in the Analysis, PepperSec's regulatory status turns on their conduct. When PepperSec acts as the developer of the dapp, its role is distinguishable from its role as an operator of the Site or from certain past actions when it retained greater control over Tornado Cash. This distinction has a material impact on the regulatory considerations for PepperSec and its future business models. The Analysis finds that, federally, there are strong arguments that PepperSec is not a money service business engaged in providing money transmission services simply by developing the dapp or hosting the Site, because it does not engage in accepting or transmitting virtual currency or otherwise interact with customer funds in either role. At the state level, this analysis holds in several states that regulated virtual currency like the federal government, but certain states are not as flexible will potentially warrant further review by PepperSec in the future.

U.S. regulators have specifically identified the provision of anonymizing software alone as insufficient to qualify a person as a money transmitter. But, where a person uses such software to provides anonymizing services, their conduct implicates money transmission laws. To that end, this Analysis also explores certain of PepperSec's past activities and future business models, seeking to highlight potential areas of risk that Dragonfly should specifically diligence prior to

[1] This Analysis does not seek to provide guidance with respect to any other regulatory frameworks that might apply to Tornado Cash or other activities, including U.S. securities laws, commodities laws. The Analysis is not a legal opinion nor is it intended to be relied on by third parties outside of Dragonfly as legal advice.

completing their investment. We conclude with a summary of our analysis, and additional thoughts on what Dragonfly might consider following up on with PepperSec.

This Analysis is divided into six parts. Part II provides a factual background of Tornado Cash, its method of operation, and relevant historical events that are pertinent for this Analysis. Part III is an overview of the federal law framework applicable to PepperSec's conduct, with a substantial focus on the BSA and the BSA Regulations. Part IV contains our core analysis of Tornado Cash and PepperSec's activities. Part V considers state money transmission laws and other state licensure requirements. Part VI summarizes our Analysis and contains our final conclusions and recommendations.

II. Facts[2]

a. Background

PepperSec is a technology services Company that has built Tornado Cash, an open source, freely available, privacy-preserving tool that uses novel cryptographic techniques to enable any participant on the Ethereum network to send and receive virtual currency in an anonymous and private fashion. Specifically, Tornado Cash enables anyone on the Ethereum network to deposit ETH and certain other virtual currencies into decentralized smart contracts that can subsequently be withdrawn by a different address. By enabling withdrawals to a new address without associating that withdrawal to the original depositor address using Tornado Cash's smart contracts, "there is **no way to link** the withdrawal to the deposit, **ensuring complete privacy.**"[3]

In addition to developing Tornado Cash, PepperSec also operates the Site, which provides a front-end user interface to facilitate access to Tornado Cash. Unlike the Tornado Cash smart contracts, which are hosted across Ethereum nodes, the primary version of the Site is privately hosted by PepperSec. However, the Site only provides a user interface to interact with Tornado Cash and is not required to access Tornado Cash itself. Savvy Ethereum users can access the smart contracts directly on the Ethereum network, bypassing PepperSec entirely if they so choose. In this manner, the Site is more of a facilitator to access Tornado Cash for less knowledgeable users rather than an inherent part of Tornado Cash itself.

The privacy functionality offered by Tornado Cash has several applications. Because transactions on most blockchain networks, including the Ethereum network, are public by default, Tornado Cash offers users an ability to transact with others without fear of their entire financial history being publicly disclosed. This assurance is crucial for widespread adoption of virtual currencies, as few people are comfortable revealing months or years of financial history to participate in daily commerce. Moreover, businesses who are increasingly interested in integrating virtual currency into their operations must presently contend with the risk of competitors monitoring and front running their business activity in the absence of privacy preserving tools like

---

[2] In the interest of time and consideration for expense, the factual summary below assumes familiarity with common cryptocurrency definitions including a blockchain, gas, the Ethereum network, ETH, etc. Where certain technical definitions are relevant to this Analysis, we provide a brief summary and refer out to other resources if the reader would like further background on these matters.

[3] *See* Tornado Cash, *Introducing Private Transactions On Ethereum NOW!*, Medium (Aug. 6, 2019), https://medium.com/@tornado.cash/introducing-private-transactions-on-ethereum-now-42ee915babe0 (the "**Launch Announcement**") (emphasis original).

Tornado Cash. Of course, just as is the case with other freely available, open source privacy tools, Tornado Cash may also be used by unscrupulous actors to engage in money laundering or other illicit activities. However, PepperSec has no ability to distinguish between or prevent certain kinds of users from accessing the Site other than IP bans, and as discussed shortly, a version of the Site is hosted independent of PepperSec or any centralized operator.

Currently, PepperSec derives no income and does not generate fees as the developer of Tornado Cash or as the operator of the Site.[4] In the future, PepperSec may generate revenue in several ways. One method may include providing additional value added services to users of Tornado Cash. Another may involve operating a Relayer (see below) and charging additional fees for the use of such services. Others still may involve providing consulting services to other ventures, or creating a digital asset to govern the operation and future development of Tornado Cash.[5]

b. Method of Operation

A full discussion of the technical elements of Tornado Cash and the cryptographic techniques it uses to preserve privacy exceeds the scope of this Analysis, but the core functions of the protocol and methods merit a brief review, as they form the core of the Tornado Cash architecture and impact PepperSec's regulatory status. In the simplest form, the Tornado Cash Protocol offers users two key functions: (i) deposits into and (ii) withdrawals from Tornado Cash smart contracts.

When a user initiates a deposit, it generates a secret message and "sends [the] hash[6] [of that message] (called a commitment) along with [the] deposit amount to the Tornado [Cash] smart contract."[7] Tornado Cash then accepts the deposit to be held in the smart contracts alongside deposits from other users, and it adds the commitment to a list of deposits that is internally tracked by the smart contracts.[8] If the user subsequently wishes to withdraw to another wallet without linkages to its original wallet, the user simply provides the Tornado Cash smart contracts with proof in the form of a signed message that it possesses a secret message associated with an unspent deposit. Once the smart contracts verify the proof, it can then transfer deposited funds to the specified address without an association to the original wallet.

---

[4] We note that we are unclear from the currently available information if PepperSec previously generated fees in excess of Ethereum network transaction fees as a Relayer and would recommend Dragonfly consider inquiring about this in diligence.

[5] Note that these are all assumptions premised off of publicly available comments from PepperSec team members, industry trends, and comparable companies.

[6] A hash in this context means the result of a cryptographic function that converts some arbitrary set of words and numbers (i.e. data related to the original deposit) into a seemingly arbitrary set of numbers. This set of numbers can be indexed in a table or other data structure in a way that associates the original set of data with the seemingly arbitrary set of numbers, and provided someone has access to the original function used to create the hash, also allows someone to quickly look up that original data by referencing only the hash. Properly done, the hashing function makes it mathematically impossible in the course of many human lifetimes (ignoring the possibility of future technology advances) to reverse engineer the original message or get the same arbitrary set of numbers for a different message.

[7] *See* Launch Announcement, *supra* note 3.

[8] For a full discussion of the mathematical formulae and applied cryptography employed in the deposit process, *see* Alexey Pertsev, Roman Semenov, and Roman Storm, *Tornado Cash Privacy Solution Version 1.4*, Tornado.cash (Dec. 17, 2019), https://tornado.cash/Tornado.cash_whitepaper_v1.4.pdf (the "**Whitepaper**").

Withdrawals can be conducted using two methods. In the first and most straightforward method, a user already possesses an Ethereum address it intends to withdraw to when it initiates a withdrawal request. In that case, once a user submits its withdrawal proof, they simply pay the network transaction fee and the deposit is released to the new wallet. However, if it is a new wallet, a circular problem emerges. That is, in order to submit a message *to* the Tornado Cash smart contracts, a user must already have received ETH *from* a wallet. If depositor uses a wallet associated with their identity (e.g. by using an exchange they have submitted identification materials to), then sending the transaction fee directly to the new wallet could undermine the entire purpose of using Tornado Cash by creating a linkage from their new wallet to the depositor.

To address this issue, Tornado Cash also allows for withdrawals using a second method, a Relayer. A Relayer essentially provides a proxy address that can pay the gas fee on behalf of a Tornado Cash user. In exchange for this service, the user pay some transaction fee to the Relayer smart contract (which should, at a minimum, be equal to at least the minimum gas fee to incentivize a Relayer to pick up the transaction), and the gas fee the Relayer pays to the Ethereum network is automatically deducted from this transaction fee chosen by the user.[9] Once the Relayer submits the gas fee and conveys the user's transmittal instructions to the Tornado Cash smart contracts, the smart contracts releases the deposit to the user's designated wallet, less the transaction fee paid to the Relayer.[10] At launch, PepperSec provided the only Relayer service,[11] but additional Relayers have since been added to enhance the robustness of the tool.

In order to ensure that an external observer cannot associate a specific deposit with a secret message when a user withdraws virtual currency, Tornado Cash employs a cryptographic technique known as Zero Knowledge Succinct Non-Interactive Argument of Knowledge ("**zk-SNARKS**"). While a full discussion of the underlying logic of zk-SNARKS is also beyond the scope of this Analysis, at its core, the idea is that zk-SNARKS provides a framework where "one can prove[12] possession of certain information, e.g. a secret key, without revealing that information, and without any interaction between the prover and verifier."[13] The "succinct" aspect of the term refers to the amount of time required to verify the information, while the "non-interactive" aspect refers to the ability of one party (i.e. the prover) to prove to another party (i.e. the verifier) the existence of the data in a single message.[14]

As of the date of this draft, "the most efficient known way to produce zero-knowledge proofs that are non-interactive and short enough to publish to a block chain is to have an initial setup phase that generates a common reference string shared between prover and verifier."[15] The

---

[9] *See* White Paper at page 1.
[10] *Id.*
[11] Note that this should be confirmed with the Company.
[12] Technically, the proof is not a mathematically formal proof, hence the reference to non-interactive "arguments" rather than non-interactive "proofs."
[13] *See* Electric Coin Co., *What are zk-SNARKS?*, Zcash https://z.cash/technology/zksnarks/ (last accessed August 23, 2020) ("**ZCash Primer**").
[14] *Id.* ("'Succinct' zero-knowledge proofs can be verified within a few milliseconds, with a proof length of only a few hundred bytes even for statements about programs that are very large. In the first zero-knowledge protocols, the prover and verifier had to communicate back and forth for multiple rounds, but in "non-interactive" constructions, the proof consists of a single message sent from prover to verifier.").
[15] *Id.*

setup phase is often referred to as a "Trusted Ceremony,"[16] and the reference string serves as the "public parameters" of the system employing a certain implementation of zk-SNARKS and are generated using "secret randomness."[17] If a person can somehow compromise the Trusted Ceremony or otherwise access or reverse engineer the randomness used to generate the reference string, they can create false proofs that would appear valid to other verifiers. By generating false proofs, they could engage in malicious activity such as generating additional units of virtual currency. In order to compromise this setup, however, an attacker "must compromise every single participant of the ceremony."[18] As such, the larger the set of participants in a Trusted Ceremony, the more difficult it will be for a malicious actor to compromise the security of the underlying system.[19] Tornado Cash uses its own implementation of zk-SNARKS that is further described in the White Paper and other publicly available materials.

c. Historically Significant Events

While we considered all facts that appeared relevant to us in preparing this Analysis, there are a few key events in PepperSec's history that transpired during the development of Tornado Cash that we believe may have lingering effects that we describe later in this Analysis. For now, we have set forth a brief timeline of relevant events below before turning back to our analysis:

- **August 6, 2019:** Tornado Cash version 1 is publicly announced and released.[20] The smart contracts deployed in connection with the launch permits only the deposit of a relatively small amount of ETH (i.e. 0.1 ETH) per transaction, and PepperSec retains an administrative key that gives them control of a multi-signature wallet where users funds are held. The administrative key also allows PepperSec to make certain smart contract changes on a unilateral basis.[21]
- **October 12, 2019**: PepperSec announces the discovery of a bug in the zk-SNARK implementation of an underlying hash function library dependency of the Tornado Cash smart contracts (the "**October 2019 Bug**").[22] The bug would have allowed a malicious attacker to drain all funds from the Tornado Cash deposit smart contract. Upon discovering the bug, PepperSec agents proactively drain all funds from the version 1 contracts themselves, deploy a set of interim smart contracts to migrate user funds to, and subject to a completed audit, the Company pledge that "the contracts will be upgraded to remove the ability for the Tornado Cash team to control the

[16] *See e.g.* Tornado Cash, *Tornado.cash Trusted Setup Ceremony*, Medium (May 1, 2020), https://medium.com/@tornado.cash/tornado-cash-trusted-setup-ceremony-b846e1e00be1 ("**Trusted Ceremony Announcement**").
[17] *See* ZCash Primer.
[18] *See* Trusted Ceremony Announcement.
[19] *Id.*
[20] *See* Launch Announcement, *supra* note 3.
[21] *See* William Foxley, *Developers of Ethereum Privacy Tool Tornado Cash Smash Their Keys*, CoinDesk (May 18, 2020), https://www.coindesk.com/developers-of-ethereum-privacy-tool-tornado-cash-smash-their-keys.
[22] *See* Tornado Cash, *Tornado.cash got hacked. By us.*, Medium (Oct. 12, 2019), https://medium.com/@tornado.cash/tornado-cash-got-hacked-by-us-b1e012a3c9a8.

contracts state and upgradability permissions will be revoked" no later than two months from the date of publication.[23]

- **December 17, 2019**: PepperSec announces Tornado Cash version 2 (the "**Version 2 Upgrade**"). The Version 2 Upgrade includes several upgrades such as higher deposit limits, support for Ethereum-based tokens, and transaction fee optimizations.[24] The Version 2 Upgrade also introduced Relayers that were not affiliated with PepperSec and removed PepperSec's administrative key upgrade functionality, although it did still retain some functionality enabling PepperSec to unilaterally provide verification key updates in anticipation of Tornado Cash's Trusted Ceremony.[25]
- **February 1, 2020**: PepperSec announces the discovery of a different bug on the user interface located at the Site (the "**February 2020 Bug**").[26] This announcement does not detail the extent of the vulnerability except to acknowledge that a small number of users were impacted, that it impacted their privacy but not the safety of their funds, and that the bug had been remedied with a post-mortem to come.[27]
- **February 13, 2020**: PepperSec supplements its February 1, 2020 announcement with a detailed breakdown of the February 2020 Bug.[28] They highlight that the February 2020 Bug involved a shareable hyperlink that could potentially expose the content of a depositor's private note, which might allow anyone who gained access to this information to withdraw unspent deposits and associate already spent deposits with withdrawal addresses.[29] However, no deposits were exposed and the bug was patched before any malicious attacker can withdraw user funds.
- **May 1, 2020**: PepperSec announces the launch of its zk-SNARKs Trusted Ceremony, publicly soliciting all interesting Ethereum network participants to participate in the ceremony to improve the long-term security guarantees of Tornado Cash.[30]
- **May 13, 2020**: PepperSec announces the conclusion of its zk-SNARKs Trusted Ceremony. With more than 1,000 participants, it becomes the largest, publicly-known Trusted Ceremony for zk-SNARKs to date. PepperSec also announces that they expect to destroy their administrative key after a few days of monitoring the performance and security of Tornado Cash.[31]
- **May 20, 2020**: PepperSec announces that it has destroyed its administrative key and set the operator address of all of its smart contracts to an address no one can access,

---

[23] *Id.*
[24] *See* Tornado Cash, *Tornado.cash version 2 has been released*, Medium (Dec. 17, 2019) https://medium.com/@tornado.cash/tornado-cash-version-2-has-been-released-8c739d3706df.
[25] *Id.*
[26] *See* Tornado Cash, *Tornado.cash vulnerability alert*, Medium (Feb. 1, 2020), https://medium.com/@tornado.cash/tornado-cash-vulnerability-alert-787e0552f950.
[27] *Id.*
[28] *See* Tornado Cash, *Vulnerability disclosure*, Medium (Feb. 13, 2020), https://medium.com/@tornado.cash/vulnerability-disclosure-f610fb7f2c8d.
[29] *Id.*
[30] *See* Trusted Setup Ceremony, *supra* note 16.
[31] *See* Tornado Cash, *The biggest Trusted Setup Ceremony in the world*, Medium (May 13, 2020), https://medium.com/@tornado.cash/the-biggest-trusted-setup-ceremony-in-the-world-3c6ab9c8fffa.

making Tornado Cash a fully permissionless protocol on the Ethereum network.[32] PepperSec also confirms that it no longer provides any Relayer functionality, with all of such functionality being provided by unaffiliated parties.[33] Further, PepperSec announces that a version of the Site has been deployed to the interplanetary file system ("**IPFS**"), a decentralized and permissionless file storage and web hosting tool that enables the deployment of front-end websites independent of a centralized web host.[34]

- **June 3, 2020**: PepperSec announces the release of a compliance tool designed to ensure that Tornado Cash users can establish provenance of funds if necessary, for commercial or legal purposes.[35]

III. Applicable Federal Law Framework

Part III of this Analysis reviews the applicable federal regime for money service businesses and certain criminal law regimes that may apply to PepperSec's activities as the creator of Tornado Cash, operator of the Site, or in certain other contexts.

a. Overview of the BSA and FinCEN

Federally, the BSA and the BSA Regulations act as key pillars of the United States' anti-money laundering ("**AML**") and counter-terrorist financing ("**CFT**") compliance framework that applies to all "financial institutions." The framework requires financial institutions to, amongst other items, register with the federal government, establish effective customer identification programs with adequate know your customer ("**KYC**") and AML processes, and observe certain disclosure, reporting, and record retention requirements. The Financial Crimes Enforcement Network ("**FinCEN**"), a division of the U.S. Department of Treasury, is the principal body that enforces the AML and CFT obligations of the BSA Regulations. FinCEN is also charged with producing implementing regulations for the BSA and providing interpretive guidance for the BSA Regulations.

The definition of a financial institution in the BSA includes a category of persons defined as "Money Service Businesses" ("**MSBs**").[36] This category includes a subset of persons known as "money transmitters."[37] Persons who qualify as money transmitters must register with FinCEN and comply with the requirements of the BSA regulations. As the definition of a "person" encompasses individuals, corporations, and "all entities cognizable as legal personalities"[38] in the BSA, the BSA Regulations have a particularly broad scope of applicability to various activities that PepperSec may be engaged in.

---

[32] *See* Tornado Cash, *Tornado.cash Is Finally Trustless!*, Medium (May 20, 2020), https://medium.com/@tornado.cash/tornado-cash-is-finally-trustless-a6e119c1d1c2.
[33] *Id.*
[34] *Id.*
[35] *See* Tornado Cash, *Tornado.cash compliance*, Medium (Jun. 3, 2020), https://medium.com/@tornado.cash/tornado-cash-compliance-9abbf254a370.
[36] 31 C.F.R. § 1010.100(t).
[37] 31 C.F.R. § 1010.100(ff)(5).
[38] 31 C.F.R. § 1010.100(mm).

The penalties for violating the BSA Regulations can be severe. By default, FinCEN may impose a range of civil penalties for failure to register as an MSB or have an adequate state license for certain regulated activities. These civil penalties typically include substantial monetary fines, but may also include prohibitions on individuals or entities from engaging in certain financial activities in the future, sometimes permanently. Certain violations of the BSA may further be criminally prosecuted by the U.S. Department of Justice (the "**DOJ**") working in concert with FinCEN as felonies. Common felonious charges for violating BSA Regulations include money laundering,[39] conspiracy to commit money laundering,[40] operating an unlicensed money transmission business,[41] and violating state laws that mandate licensure of certain financial institutions. All of these crimes may be punished with imprisonment and severe criminal monetary penalties, which are often exponentially larger than civil penalties due to their punitive intent.

i. Federal Regulation of Money Transmission and Virtual Currency Technology

The BSA Regulations include "money transmitters" as MSBs. Money transmitters are persons providing "money transmission services," or otherwise engaged in the transfer of funds.[42] Money transmission services involve "the acceptance of currency, funds, *or other value that substitutes for currency* from one person **and** the transmission of currency, funds, or *other value that substitute for currency* to another location or person by any means."[43] These broad definitions provide FinCEN with wide flexibility in applying the BSA Regulations, regardless of corporate form or the use of novel technology. Whether a person constitutes a money transmitter is therefore "a matter of facts and circumstances" [44] that requires an analysis of a person's proposed activities rather than their corporate status or nomenclature used.

The BSA also includes exempt categories of persons that do not constitute money transmitters, even when they provide the means for others to engage in money transmission services or engage in the transfer of value themselves. Relevant for purposes of this Analysis are two specific exemptions. First, persons who merely provide the "delivery, communication, or network access services used by a money transmitter to support money transmission services" are exempt from qualifying as money transmitters (hereinafter referred to as the "**Developer Exemption**").[45] Second, a person will not be a money transmitter if they "accept and transmit funds only integral to the sale of goods or the provision of services, other than money transmission services, by the person who is accepting and transmitting the funds" (hereinafter referred to as the "**Integral Exemption**").[46] As discussed further below, these exemptions reflect FinCEN's focus on regulating those engaged in providing money transmission services rather than those who merely provide the software or other means to do so.

---

[39] 18 U.S.C. § 1956(a).
[40] 18 U.S.C. § 1956(h).
[41] 18 U.S.C. § 1960(a).
[42] 31 C.F.R. § 1010.100(ff)(5)(i).
[43] 31 C.F.R. § 1010.100(ff)(5)(emphasis added).
[44] *Id.*
[45] 31 C.F.R. § 1010.100(ff)(5)(ii)(A)
[46] 31 C.F.R. § 1010.100(ff)(5)(ii)(F)

The BSA Regulations are expansive, and FinCEN recognized that understanding their application can be challenging for market participants dealing with virtual currency. To that end, FinCEN has promulgated interpretive guidance in addition to its enforcement activity to further delineate the application of the BSA to virtual currency activities. The two most relevant pieces of guidance for purposes of this Analysis are two reports produced by FinCEN in 2013 and 2019, respectively.

ii. 2013 Virtual Currency Guidance

In 2013, FinCEN issued interpretative guidance seeking to clarify the applicability of BSA Regulations to virtual currencies (the "**2013 Virtual Currency Guidance**").[47] There, FinCEN distinguished between real currency, and virtual currency, defining the latter as a "medium of exchange that operates like a real currency in some environments, but does not have all the attributes of real currency," including status as legal tender.[48] Further, FinCEN emphasized that the 2013 Virtual Currency Guidance applied solely to *convertible* virtual currencies ("**CVC**"), which it defined as a "type of virtual currency [that] either has an equivalent value in real currency, or acts as a substitute for real currency."[49]

While FinCEN failed to provide further examples of what type of virtual currency would qualify as a CVC in the 2013 Virtual Currency Guidance, later guidance from the Financial Action Task Force ("**FATF**")[50] helped clarify the distinction between convertible and non-convertible virtual currencies. FATF's guidance is not binding legislation within the U.S., but its definition aligns with FinCEN's approach and was shaped in part by U.S. regulators as active members of FATF. In its guidance, FATF defines CVCs, such as Bitcoin, as virtual currencies that have "equivalent value in real currency and can be exchanged back-and-forth for real currency."[51] Non-convertible virtual currencies, such as Amazon credits, are considered virtual currencies that are "intended to be specific to a particular virtual domain or world…and under the rules governing its use, cannot be exchanged for fiat currency."[52] For purposes of this Analysis, we have assumed that the 2013 Virtual Currency Guidance is relevant to PepperSec, because Tornado Cash uses virtual currencies that are widely recognized as CVCs by FinCEN, such as ETH.

The 2013 Virtual Currency Guidance established a tripartite framework for classifying CVC market participants. Persons transacting in CVCs are categorized as "users," "exchangers," or "administrators." Users are persons who obtain CVC to purchase goods and services on their own behalf (and not as a business or for the accounts of others) and are not MSBs under the BSA.[53] On the other hand, exchangers are defined as persons "**engaged as a business** in the exchange of

---

[47] *See* FIN-2013-G001, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (Mar. 18, 2013), *available at* https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.
[48] *Id.* at 1.
[49] *Id.*
[50] The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes global money laundering and terrorist financing policies. While FATF does not produce binding legislation, FATF guidance and recommendations are broadly recognized as global AML and CFT standards, and member states often implement legislation in line with the entity's recommendations. Their guidance is thus instructive with respect to how member states may define assets within their own body of law.
[51] *See*, Financial Action Task Force, *Virtual Currencies – Key Definitions and Potential AML/CFT Risks*, 4 (2014), https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.
[52] *Id.*
[53] *See* 2013 Virtual Currency Guidance, *supra* note 47 at 2.

virtual currency for real currency, funds, or other virtual currency,"[54] and administrators are defined as persons "**engaged as a business** in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency."[55] Unlike Users, if either an Exchanger or an Administrator "(i) accepts and transmits [CVC] or (ii) buys or sells [CVC] for any reason," they are deemed to be money transmitters subject to the BSA Regulations, unless an applicable exemption applies.[56]

iii. 2019 Virtual Currency Guidance

Following publication of the 2013 Virtual Currency Guidance, FinCEN and its representatives issued several administrative orders and public statements to provide further guidance.[57] And, in 2017, FinCEN, in conjunction with the DOJ, announced one of the largest enforcement orders against the exchange BTC-E, highlighting the applicability of the BSA to CVC businesses.[58] However, market confusion remained about the applicability of the BSA regulations, and in response to sustained inquiries from market participants, on May 9, 2019, FinCEN produced additional interpretative guidance (the "**2019 Virtual Currency Guidance**").[59] The 2019 Virtual Currency Guidance was not intended to supplant the 2013 Virtual Currency Guidance, but instead supplements it by consolidating previous guidance and applying FinCEN's regulatory framework to several examples of common CVC business models.

The 2019 Virtual Currency Guidance emphasized FinCEN's substantive approach of focusing on the facts and circumstances of a person's *activities* with CVC. It clarified that, irrespective of what order CVC is accepted or transmitted, or whether one or more CVCs are exchanged, exchangers and administrators who accept and transmit CVC will still qualify as money transmitters absent an available exemption.[60] It further clarified that such persons were engaged in money transmission regardless of whether they accept and transmit CVC repeatedly

---

[54] *Id.* (emphasis added).
[55] *Id.* (emphasis added).
[56] *Id.* at 3.
[57] For instance, in 2014, FinCEN held that a company making investments in virtual currency by producing and deploying software where virtual currency holders could initiate a process to sell virtual currency to the company did not qualify as a money transmitter. FinCEN Ruling 2014-R002, *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity* (Jan. 30, 2014), https://www.fincen.gov/sites/default/files/shared/FIN-2014-R002.pdf. In another 2014 action, FinCEN found that a company operating a convertible virtual currency trading book and platform with custodial accounts was a money transmitter. FinCEN Ruling 2014-R011, *Request for Administrative Ruling on the Application of FinCEN's Regulation to a Virtual Currency Trading Platform* (Oct. 27, 2014). *See* also, Letter from Drew Maloney, Assistant Sec'y, US Dep't of the Treasury, to Senator Ron Wyden, US Senate Comm. on Fin. (Feb. 13, 2018).
[58] *See, IN THE MATTER OF: BTC-E a/k/a Canton Business Corporation and Alexander Vinnik*, No. 2017-03, Assessment of Civil Money Penalty (July 26, 2017), https://www.fincen.gov/sites/default/files/enforcement_action/2020-05-21/Assessment%20for%20BTCeVinnik%20FINAL2.pdf.
[59] *See* FIN-2019-G001, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (May 9, 2019), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf (the "**2019 Virtual Currency Guidance**").
[60] *Id.* at 8.

on an account basis, in one-off transactions, or only on conditional terms pursuant to predetermined conditions.[61]

These general principles, together with FinCEN's recognition that certain activities warrant exemption from the application of the BSA Regulations, serve as the bedrock for FinCEN's analysis in the 2019 Virtual Currency Guidance. The result is a framework that distinguishes between those who provide the means that enable others to engage in money transmission on the one hand, and business or platform-operators that actually provide money transmission services using these means on the other. As described further below, they specifically recognized this distinction applying in the context of anonymity-enhanced CVC activity. Accordingly, the fact that PepperSec may not qualify as a money transmitter in a developer context does not necessarily mean that PepperSec is not a money transmitter in another context as a business or platform-operator.

IV. Federal Law Analysis

a. *Development of Tornado Cash Alone Does Not Constitute Money Transmission Because PepperSec's Development Activity Qualifies for the Developer Exemption*

In the 2019 Virtual Currency Guidance, FinCEN established a taxonomy for analyzing anonymity-enhanced CVC transactions ("**Private Transactions**"). They categorized these transactions as either (i) transaction denominated in ordinary CVC (e.g. Bitcoin) but structured in a way to mask information that would normally be publicly viewable by default on a public ledger or (ii) transactions denominated in CVC specifically designed to prevent tracing (i.e. privacy coins like Monero).[62] They further distinguished between anonymizing **services** providers and anonymizing **software** providers.[63]

Anonymizing services providers are engaged in providing money transmission services, as they accept and transmit CVCs on behalf of users. However, anonymizing software providers do not qualify as money transmitters, as they only provide the means for money transmit***tors*** (i.e. those who merely provide transmittal instructions to money transmitters) to submit transmittal instructions that a money transmit***ter*** must execute and are therefore eligible for the Developer Exemption.[64] Whether PepperSec qualifies as a money transmitter is thus dependent on what role PepperSec occupies in the Private Transactions conducted by Users through Tornado Cash.

---

[61] *Id.* ("[A] person may be a money transmitter when operating either on a transactional basis or on an account basis…[and] a person will qualify as a money transmitter if that person accepts value with the intent of transmitting it only under certain conditions.").

[62] *Id.* at 18 ("Anonymity-enhanced CVC transactions are transactions either (a) denominated in regular types of CVC, but structured to conceal information otherwise generally available through the CVC's native distributed public ledger; or (b) denominated in types of CVC specifically engineered to prevent their tracing through distributed public ledgers (also called privacy coins).").

[63] *Id.* at 19 ("Providers of anonymizing services, commonly referred to as "mixers" or "tumblers," are either persons that accept CVCs and retransmit them in a manner designed to prevent others from tracing the transmission back to its source (anonymizing services provider), or suppliers of software a transmit***tor*** would use for the same purpose (anonymizing software provider).").

[64] *Id.* at 3 ("FinCEN's regulations define the term "money transmitter" to include a "person that provides money transmission services," or "any other person engaged in the transfer of funds." A "transmittor," on the other hand, is "[t]he sender of the first transmittal order in a transmittal of funds…In other words, a transmit***tor*** initiates a transaction that the money transmit***ter*** actually executes.")(emphasis original).

As the developer of Tornado Cash smart contracts, PepperSec acts as an anonymizing software provider and has strong arguments that they qualify for the Developer Exemption. Tornado Cash does not entail PepperSec accepting and retransmitting any CVC on behalf of Tornado Cash users, as it is completely noncustodial and PepperSec has no ability to access the underlying funds or to change the parameters of the smart contract to effectuate the transmission of user's funds. Rather, Tornado Cash is precisely the type of Private Transaction software FinCEN identified as providing the means for money transmitt***ors*** (i.e. Tornado Cash users) to provide privacy enhanced transmittal instructions to Ethereum network.[65]

In addition, another section of the 2019 Virtual Currency Guidance unrelated to Private Transactions generally established that, "the developer of a [da]pp is not a money transmitter for the mere act of creating the application, even if the purpose of the [da]pp is to issue a CVC or otherwise facilitate financial activities denominated in CVC."[66] This exemption also traces its roots to the Developer Exemption in that FinCEN reasoned that developers creating dapps are engaged in the production of goods and services rather than money transmission itself.[67] Accordingly, whether it is as a general dapp developer or as an anonymizing software provider, we believe PepperSec has strong arguments that mere development of Tornado Cash is insufficient to require registration as a federal MSB.

b. *Development and Hosting of the Site Does Not Constitute Money Transmission because PepperSec is Merely Providing a Means to Access Tornado Cash Smart Contracts*

The development of the Site alone is unlikely to trigger money transmission concerns. As described above, FinCEN permits the unlicensed development of anonymizing software provided that the developer does not use such software to engage in money transmission services, and the developers of dapps alone are not money transmitters. Therefore, even if the Site were to be considered an integral part of Tornado Cash, development of the Site would not constitute money transmission.

Operation of the Site is also unlikely to constitute money transmission itself, although it does increase the risk of separate money laundering liability concerns we describe separately in this Analysis. Even as the operator of the Site, PepperSec does not actually accept or transmit user funds. The front end provides one method to access the Tornado Cash smart contracts, but users are not obligated to use this interface. Experienced users can interact directly with the Tornado Cash smart contracts. Alternatively, users can access a version of the user interface directly on the Ethereum network that is hosted on IPFS and not subject to control by PepperSec. The various ways to interact with Tornado Cash in conjunction with – or independent of – PepperSec highlights the fact that PepperSec is not providing money transmission services or operating Tornado Cash

---

[65] *Id.* at 20 ("An anonymizing software provider is not a money transmitter. FinCEN regulations exempt from the definition of money transmitter those persons providing "the delivery, communication, or network access services used by a money transmitter to support money transmission services." This is because suppliers of tools (communications, hardware, or software) that may be utilized in money transmission, ***like anonymizing software***, are engaged in trade and not money transmission.") (emphasis added).

[66] *Id.* at 27.

[67] *Id.*

itself when it provides access to the Site. Instead, PepperSec provides just one of several services that can be used to access Tornado Cash as a dapp, and we believe there are therefore strong arguments that the Site's development and operation similarly qualify for the Developer Exemption.[68]

c. *Tornado Cash May Constitute a Money Transmitter Dapp that is Independent of PepperSec*

In the 2019 Virtual Currency Guidance, FinCEN stated that, "when [da]pps perform money transmission, the definition of money transmitter will apply to the [da]pp, the owners/operators of the [da]pp, or both."[69] The framework FinCEN applies in assessing dapps is the same framework they apply to operators of CVC kiosks (e.g. Bitcoin ATMs). FinCEN defines CVC kiosks as "electronic terminals that act as mechanical agencies of the owner-operator, to enable the owner-operator to facilitate the exchange of CVC for currency or other CVC," and to the extent that an operator uses the electronic terminal "to accept currency from a customer and transmit the equivalent value in CVC (or vice versa),"[70] they are engaged in money transmission. This conclusion obtains irrespective of whether the CVC being exchanged is the owner-operator's or is coming from a third party site as a result of a real-time exchange.[71]

It is possible that FinCEN would view the Tornado Cash smart contracts themselves as a dapp engaged in money transmission services. According to PepperSec themselves, the deposit contract plainly accepts CVC from depositors for storage, and subsequently transmits CVC on behalf of those depositors to other persons or locations. As such, the Tornado Cash smart contracts do appear to qualify for money transmission services. Further, FinCEN has stated that "persons who accept and transmit value in a way ostensibly designed to protect the privacy of the transmitt*or* are providers of secure money transmission services and are not eligible for the [I]ntegral [E]xemption," because secure money transmission services are not a distinct business from generally providing money transmission services, and the Integral Exemption requires that distinction.[72]

Notwithstanding the above, we believe PepperSec is distinguishable from operators of CVC kiosks and has better arguments that it is not an owner-operator of Tornado Cash in the same style of an owner-operator of a CVC kiosk. Unlike owner-operators of CVC kiosks, PepperSec does not own Tornado Cash (i.e. anyone can access the publicly available source code and redeploy it on IPFS under the terms of an open source license), operate it for its own benefit, or otherwise generate revenues from operating and owning the Site. They have no ability to maintain, modify or upgrade the platform after burning their administrative key, and future iterations of Tornado Cash would require that users elect to opt into the new smart contracts. In contrast, owner-operators

---

[68] We reiterate here that PepperSec does not derive revenue from the Site, suggesting that it is not **engaged as a business** in providing services, even if operation of the Site were to somehow qualify as providing money transmission services.
[69] *See* the 2019 Virtual Currency Guidance, *supra* note 47 at 18.
[70] *Id.*
[71] *Id.*
[72] *Id.* at 19 (discussing a prior administrative order wherein FinCEN rejected an applicant's claim that providing a service which accepted and transmitted value for transmittors in a way designed to preserve their privacy alone was providing security services separate from secured money transmission).

of CVC kiosks unilaterally control access to their kiosks, are responsible for their upkeep, and they can modify them to the extent legally permissible. Even as it conceptualized its own definition of a dapp, FinCEN recognized that, "[g]enerally, a [da]pp user must pay a fee to the [da]pp **(for the ultimate benefit of the owner/operator)** in order to run the software,"[73] and they specified that *either* or *both* of a dapp and its owner-operator may qualify as money transmitters.

It is unclear what outcome may obtain if our Analysis holds and Tornado Cash as a dapp is considered a money transmitter while PepperSec as its developer qualifies for applicable exemptions. There is no precedent for such an assessment, but we expect that should they take issue with Tornado Cash, FinCEN might strongly dissuade PepperSec from deploying future iterations of Tornado Cash under the specter of threatening potential money transmitter violations before pursuing formal action, as they may wish to avoid setting bad precedent with a losing case if this theory does not hold. It would then be incumbent on PepperSec to decide whether it wished to continue to proceed with their development efforts, although we believe recent actions, such as the development of their compliance tool, suggest that PepperSec could continue developing a version of Tornado Cash that ensures privacy but allows money transmitters transacting with Tornado Cash users to meet their BSA obligations. Further, while a constitutional discussion is not the subject of this Analysis, PepperSec may have compelling arguments that FinCEN would infringe its First Amendment rights by compelling them to cease development of a free, open-source tool.[74]

If Dragonfly elects to move forward with an investment, we believe that you should prioritize understanding what future iterations of Tornado Cash will look like in diligence, and critically, what revenue sources PepperSec is considering, because both of these factors may increase the risk of collapse in the distinction between Tornado Cash the dapp and PepperSec the developer. While we believe they may have multipronged arguments as outlined above, if the key consideration for whether PepperSec as a money transmitter is whether they're engaging in commercial activity, then a path towards long-term profitability may elude them without substantial structural changes. Whether such changes can be implemented while preserving the unique value proposition of Tornado Cash is a determination we defer to the reader and the PepperSec team.

d. *Prior Conduct by PepperSec May Have Constituted Money Transmission Services*

---

[73] *Id.* at 18 (emphasis added).

[74] While the adage "code is speech" has often been misinterpreted as an unfettered right to propagate software code with no oversight or restraint, it is rooted in actual case law that may be relevant for PepperSec. Specifically, in *Bernstein v. US Dept. of State*, 922 F. Supp. 1426 (N.D. Cal. 1996) ("**Bernstein**"), the court recognized that source code, including "functional" source code, could be expressive speech for purposes of the First Amendment and may therefore be entitled to protection from unlawful government restraint. In that case, coincidentally, the plaintiff wished to publish a paper along with an encryption algorithm and the underlying source code related to the algorithm, but export laws required that he submit his work to, register with, and obtain special licenses from the U.S. government prior to doing so. The plaintiff, represented by attorneys from the Electronic Frontier Foundation, argued that this was an unlawful restraint on his First Amendment right of expression, and the team eventually secured a victory on First Amendment grounds when the court likened source code production to other unorthodox forms of expression. This led to the U.S government materially changing its export regulation requirements and leading to the now oft misrepresented "code is speech" proverb.

Although the current iteration of Tornado Cash appears to have sound legal arguments and demonstrate good faith efforts to ensure compliance with applicable law, certain of their prior actions may have, individually or in the aggregate, created yet unrealized liabilities that could pose enforcement risk in the future. Specifically:

- **Administrative Key and Multi-Signature Wallet Control**: Until at least May 2020, PepperSec retained control of an administrative key that gave it emergency access to user funds in the event of a failure, allowed upgradeability of Tornado Cash smart contracts, and gave it control of other critical smart contract features. This unilateral control may have created potential liability under the BSA, as FinCEN may allege that the ability to move user funds alone sufficed to constitute money transmission, but this argument is lacking. Even if we assume that the administrative key could move user funds arbitrarily, we are unaware of any prior cases or enforcement actions conducted by FinCEN where the mere ability to touch user funds alone without actually engaging in money transmission services has been found sufficient to make that person a money transmitter.

  However, the multi-signature wallet *actually* used by PepperSec prior to the completion of its Trusted Ceremony and transition to a fully permissionless system poses more risk. Because PepperSec was in sole control of the multi-signature wallet until May 2020, any user funds deposited there were ultimately subject to their sole control. During this interim period then, the Tornado Cash wallet holding user funds may have qualified as a "hosted wallet" (i.e. custodial) under the 2019 Virtual Currency Guidance. Hosted wallet providers are considered money transmitters, and while multi-signature wallet service providers are exempt from a similar classification, that exemption requires that the multi-signature wallet provider be providing additional verification on behalf of users rather than itself.

  Dragonfly might consider asking for further details about the administrative key and multi-signature wallet as part of its due diligence process, particularly with respect to any actions that *have not* been publicly announced and may have implicated user funds. If it wished to take an aggressive stance, requesting a special indemnity for any liability that might arise in connection with PepperSec's activity operating the multi-signature wallet and holding the administrative key could provide the fund with extra protection, but PepperSec may balk at the request.

- **The October Bug and the Version 2 Upgrade**: As described in Part II, the Company responded to a critical bug in October 2019 by withdrawing user funds and moving them to another set of smart contracts before ultimately deploying them to a third set of smart contracts in connection with the Version 2 Upgrade. Unlike mere development activity, this activity may be viewed as providing money transmission services as an Exchanger, because PepperSec previously accepted funds into smart contracts they controlled (by virtue of owning the administrative key to the multisignature wallet where funds were held) and later transmitted those funds to another set of smart contracts. Further, as mentioned above, the

multisignature wallet used by the company at the time may constitute a "hosted wallet" that held all user funds under the 2019 Virtual Currency Guidance.

Dragonfly might consider asking for further details about this migration, whether any regulators have reached out in connection with the October 2019 Bug or the Version 2 Upgrade, and, if it wished to take an aggressive stance, request a special indemnity for any liability that might arise in connection with PepperSec's activity in connection with the October 2019 Bug, but PepperSec may balk at the request.

- **Relayer Activity:** During the launch phase of Tornado Cash and until at least December 17, 2019, it appears that PepperSec provided the sole Relayer service. It is possible that FinCEN would allege that the Relayer service, unlike development activity, entails more than just providing the means for money transmitters or users to engage transactions. Rather, they might allege that the Relayer service involved actually accepting funds from users and transmitting them to another person or location (i.e. the recipient).

  This allegation is less likely to obtain relative to other allegations FinCEN may set out, because no Relayer actually has access to user funds based on our understanding of Tornado Cash's infrastructure. Rather, the Relayer only accepts instructions from a user and prepays the gas transaction fee *to the Ethereum network miners* on behalf of the requesting user so that the Tornado Cash smart contracts can release funds to the requesting user. In this sense, we think it more appropriate to view the Relayer as akin to a money transmitt***or***, because they provide the first set of instructions to the Tornado Cash smart contracts to release previously accepted funds to the user (users cannot submit these instructions absent the requisite transaction fee being paid to the network).

- **February 2020 Bug**: Also as described in Part II, the Company responded to a bug in February 2020 by upgrading the user interface for the Site. Unlike their response to the October 2019 Bug, PepperSec did not take any possession of user funds or exercise any control of their administrative keys. Instead, PepperSec modified the back-end operation of the Site and redeployed it.

  Assuming our analysis that operation of the Site alone does not qualify as money transmission obtains, we believe that PepperSec's response to the February 2020 Bug does not pose more material risk than most of their prior actions (excluding the October 2019 Bug and control of the original multi-signature wallet). Their conduct in this event consisted solely of modifying the means in which people can access Tornado Cash on the Site, which would appear to remain subject to the Developer Exemption, since PepperSec is merely modifying the means in which money transmitt***ors*** (i.e. users and Relayers) interact with Tornado Cash. Moreover, users could continue to access Tornado Cash directly on the Ethereum network without being exposed to this bug.

We note that, in the event any of the aforementioned risk areas are realized, the Integral Exemption is unlikely to provide a reliable exemption for PepperSec to consider. As referenced previously in this Analysis, FinCEN does not view providing secured money transmission services as a sufficiently distinct business from typical money transmission services and has therefore rejected applying the Integral Exemption in similar contexts.

If PepperSec was engaged in any or all of the above activities (or had the ability to do so), the risk of a potential enforcement action would likely increase, because they suggest that they are not just developers of Tornado Cash, but the operators providing money transmission services. However, it appears to us that they have largely removed any ability from them to engage in this future activity. Whether FinCEN will pursue them for prior actions is unpredictable, and while the agency is frequently willing to work with developers, privacy preserving technology is often subject to more scrutiny and less sympathy due to the common assumption that such technology can thwart law enforcement efforts. Because statutes of limitations on most claims referenced in this Analysis are at least 5 years, absent requesting a no action letter from FinCEN, risks described above may persist through 2025 at the earliest.

e. *PepperSec May Still be Subject to Money Laundering Liability Risk*

In concluding this review of applicable federal law, we also highlight that, irrespective of PepperSec's status as a money transmitter, criminal penalties for money laundering and related crimes may obtain. Money laundering requires the intent to process criminally obtained proceeds in a manner that obfuscates their illegal source. While PepperSec might plausibly argue that it cannot possibly know whether any particular user's source of funds has been obtained illegally or that such user is using Tornado Cash to engage in criminal conduct, the U.S. government has been surprisingly aggressive in pursuing certain cryptocurrency related violations.[75] It is foreseeable that they could – not unreasonably – allege that PepperSec knows that some percentage of transactions conducting on Tornado Cash will necessarily have tainted funds, because there have been public reports of malicious actors using the platform to cleanse funds following hacks,[76] and PepperSec itself has provided tutorials on how to more effectively use Tornado Cash to preserve privacy.[77] And, in February of this year, the Department of Justice brought suit against an individual providing mixing services, charging them with money laundering conspiracy, operating an unlicensed money transmitter business, and engaging in money transmission without a state license (the "**Harmon Case**").[78]

---

[75] *See* Daniel Palmer, *Ethereum Developer Virgil Griffith Indicted Over North Korea Event Appearance*, CoinDesk (January 9, 2020), https://www.coindesk.com/ethereum-developer-virgil-griffith-indicted-over-north-korea-event-appearance.

[76] *See e.g.*, Messari, *DeFi faces another high-profile attack as Balancer loses $500K*, Messari.io (June 29, 2020), https://messari.io/article/defi-faces-another-high-profile-attack-as-balancer-loses-500k (noting that a hacker immediately moved funds to Tornado Cash following an attack to cleanse the proceeds).

[77] *See* Tornado Cash, *How to stay anonymous with Tornado.cash and similar solutions*, Medium (Jan. 3, 2020), https://medium.com/@tornado.cash/how-to-stay-anonymous-with-tornado-cash-and-similar-solutions-efdecdbd7d37.

[78] *See* Department of Justice, Office of Public Affairs, *Ohio Resident Charged with Operating Darknet-Based Bitcoin "Mixer," which Laundered Over $300 Million*, The United States Department of Justice (Feb. 13, 2020), https://www.justice.gov/opa/pr/ohio-resident-charged-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million.

However, while PepperSec has a non-zero risk of exposure to money laundering risk, we believe there are reasonable grounds to view them as qualitatively different from instances like the Harmon Case. In the Harmon Case, the defendant operated a custodial mixer as a for profit enterprise to conceal illicit transactions on the darknet.[79] In contrast, PepperSec has no access to user funds, does not operate Tornado Cash as a business, and has no insight into who uses the tool. Further, our prior discussion established that PepperSec has strong arguments that its current activities do not constitute money transmission activities under the 2019 Virtual Currency Guidance. The defendant in the Harmon case clearly accepted and transmitted funds on an ongoing basis to enrich themselves. And, PepperSec may

As before, PepperSec's prior actions may create slightly more risk in this regard. For instance, when the multi-signature wallet was controlled by the company, the aforementioned arguments lose some potency. If PepperSec was actually engaged in money transmission when it transferred funds as part of the V2 Upgrade, or if it was publicly known that criminal proceeds were being laundered through Tornado Cash at that time, there may be grounds for the DOJ to argue that PepperSec facilitated or conspired to facilitate money laundering. While PepperSec cannot mitigate actions that have already transpired, we would expect that they would seek to refrain from similar conduct to reduce the likelihood of grappling with these issues.

V. Applicable State Law

Nearly every U.S. state[80] and territory regulates money transmission activity separate from the BSA Regulations and requires state-specific licenses to provide money transmission services to their residents. Each jurisdiction has the authority to interpret its own law and vary in their definitions, but almost all generally cover entities that act as intermediaries between parties to a transaction who receive money for transmission or otherwise transfer "monetary value"[81] between one person or location and another. States have taken different approaches with respect to virtual currency. These actions span the gamut, from establishing entirely new regulatory regimes (e.g., New York), to incorporating virtual currency activities into the already existing state money transmission laws, to offering little or no guidance.[82] Others still have taken the view that their

---

[79] *See Id.*

[80] Montana does not currently regulate money transmission.

[81] The application of state laws to virtual currency has led to an assortment of court decisions in different jurisdictions. For example, in the *Florida v. Espinoza*, the State of Florida charged Espinoza with two counts of money laundering and one count of unlawfully engaging as an MSB. In that instance, Espinoza posted to online forums to sell bitcoin for cash and arranged local meetings where he would provide them with instructions on where to deposit the Bitcoin in exchange for the cash. Espinoza was arrested charged after undercover law enforcement made two purchases from him. In response to Espinoza's motion to dismiss, the Circuit Court of Florida's Eleventh Judicial Circuit held that Espinoza's activities did not violate the law because the Espinoza was a seller, as opposed to a middleman, in a transaction for the transfer of money from one person to another. With respect to the money laundering claim, the Court found that bitcoin was not a monetary instrument and therefore not money laundering. *See* Order Granting Defendant's Motion to Dismiss the Information, *State v. Espinoza*, F14-2923 (Fl. 11th Cir Ct. Jul. 22, 2016).

[82] *See*, e.g., Ca. Fin. Code §§ 2000 et seq., N.Y. Banking Law §§ 640 et seq., Tex. Fin. Code §§ 151.201 - 151.860. See also Nat'l Money Transmitters Ass'n, State-by-State Regulation.

money transmission laws do not apply to CVC at all, because they do not constitute money or "monetary value."[83]

While the application of state laws to virtual currencies varies, licensing requirements are fairly consistent and may include:

- Submission of personal history, personal financial statements and credit records of officers, directors, and 10% or more shareholders ("**Control Persons**");
- Audited financial statements of the company and any parent or subsidiaries, including evidence of minimum tangible net worth/capital;
- Obtaining surety bonds in each state;
- A detailed business plan outlining product, targets markets, projections, and fee schedule;
- Criminal and civil background checks on Control Persons performed by a third-party, including fingerprinting; and
- Listing all civil and criminal complaints and regulatory actions brought against a Control Person for some period of time prior to application.

Each state's money transmission laws would need to be considered in light of the facts and circumstances of PepperSec's activity and Tornado Cash to determine if a license is required. A full analysis of each state's laws is beyond the scope of this Analysis, but key principles can be broadly derived.

In states where CVCs are subject to money transmission laws, the analysis is often similar to an analysis under the previously described federal framework. That is, whether a person constitutes a money transmitter typically turns on the role it plays in accepting and transmitting value between participants to a transaction. Where a person serves as an intermediary and holds funds on users' behalf for distribution, their activities may constitute money transmission. Conversely, where a person merely provides instructions or develops software that others use to engage in money transmission, money transmission is not typically found.

From this perspective, PepperSec's activity as a mere developer of Tornado Cash or making the Site publicly available may not constitute money transmission under many states' laws. But certain states may still view the operation of the Site as money transmission, and certain past or future activities, such as PepperSec's response to the October 2019 Bug or future business models wherein they are generating revenue from the operation of the Site, may be viewed by some state regulators as money transmission. Further, every state does not have a corresponding exemption to the Developer Exemption, unlike at the federal level. As such, while we believe that

---

[83] *See* Texas Department of Banking, Supervisory Memorandum – 1037, *Regulatory Treatment of Virtual Currencies under the Texas Money Services Act* (Apr. 1, 2019) ("Because cryptocurrency is not money under the Money Services Act, receiving it in exchange for a promise to make it available at a later time or different location is not money transmission."), https://www.dob.texas.gov/public/uploads/files/consumer-information/sm1037.pdf. We note, however, that stablecoins backed by sovereign currency such as USDC may receive different treatment in these regimes.

their activities pass muster in several states, a detailed analysis of each would be warranted for greater assurance.

One unique jurisdiction warranting separate mention is the state of New York. In addition to having a money transmission framework, New York has also passed legislation specific to regulating virtual currencies.[84] This legislation, known as the BitLicense, provides New York state regulators with an expansive scope of authority. This authority includes the authority to regulate any person "receiving [v]irtual [c]urrency for [t]ransmission or [t]ransmitting [v]irtual [c]urrency" or persons "storing, holding, or maintaining custody or control of [v]irtual [c]urrency" on behalf New York residents. While certain exemptions may apply, including an exemption for developers of software alone,[85] New York regulators have adopted a broad view of their mandate under the Bitlicense. As such, PepperSec should consider whether it wishes to IP ban New York internet protocol addresses out of an abundance of caution, since those activities may create obligations to register and observe the compliance requirements of the Bitlicense, in addition to certain state's money transmission rules. If future activities hew more closely to traditional money transmission, we would recommend PepperSec working closely with counsel before offering engaging in those activities in the state of New York.

VI. Summary and Conclusion

Federally, PepperSec has strong arguments that it is not a money transmitter from several perspectives. As the creator of Tornado Cash, it is acting in a software developer capacity and engaged in trade. It does not provide services as an Exchanger or an Administrator in this capacity, and such activities should fall within the Developer Exemption, as FinCEN specifically identified this type of anonymizing software provider as being eligible to avail itself of the Developer Exemption in the 2019 Virtual Currency Guidance. As the platform-operator of the Site, it is not responsible for accepting or transmitting funds. And, since May 2020, it has had no ability to modify the underlying smart contracts for Tornado Cash. These models should therefore fall outside of the scope of FinCEN's regulatory authority.

If certain activities were to potentially implicate the BSA Regulations, prior actions (and any future actions or business models) entailing PepperSec's control of user funds or Tornado Cash itself appear most apt to be the culprit. In those instances, PepperSec may have acted in a custodial capacity for users and not simply as a developer, but as the manager of a secured money transmission service. Future business models may be less fraught with compliance issues but should still be assessed against the framework described herein.

As PepperSec considers monetizing it's technology, relevant questions pertaining to how it will generate revenue become critical, because the categorization of an actor or potential liability often turns on whether it is engaged in conducting business or merely personal consumptive

---

[84] 23 NYCRR Part 200.

[85] *See* New York State Department of Financial Services, *Bitlicense Frequently Asked Questions* (last accessed June 13, 2019) ("**Do I need a BitLicense simply to develop software?** No. The development of software in and of itself does not require a BitLicense."), https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses/bitlicense_faqs.

activity. In particular, to the extent that any business plan involves (i) custody of user funds, (ii) charging fees on transactions with a high probability of having a criminal source of proceeds, or (iii) operating a Relayer for profit, we would strongly encourage the company to discuss its plans with their counsel, as these appear to be potential areas where fees can be generated but that may also have material impacts on their legal status.

Although this Analysis does not purport to provide a thorough state-by-state analysis, the aforementioned analyses remain largely applicable at the state level where CVCs are regulated in line with the federal approach. However, where there may be the Developer Exemption available at the federal level, all states do not similarly provide for analogous exemptions. Even where PepperSec is comfortable proceeding on a federal level and in most states then, they should specifically consider states like New York, which may have more stringent legislation applicable to virtual currency operators.

For Dragonfly, we would recommend that, at a minimum, you leave the diligence process with (i) a comfortable understanding of Tornado's past actions and any unannounced activity of a similar kind, if applicable, (ii) a high-level sense of long-term monetization possibilities and whether they can be accomplished without implicating the issues highlighted in this Analysis, (iii) knowledge about what other compliance efforts the team can integrate if a regulator attempted to compel further amendments to Tornado Cash. This would equip the fund with relevant facts to assess its comfort with potential legal risk for the foreseeable future, but also to potentially assess the likelihood of large-scale growth without putting PepperSec's principals at risk or become subject to regulatory enforcement actions.

To mitigate future risks, PepperSec could ultimately elect to register with FinCEN and seek licensure from relevant states, or it could instead elect to restrict the availability of Tornado Cash from certain users. However, it is unclear to us that PepperSec could meet BSA obligations, or that it can reliable prevent access to any user since it does not host the sole access point to the Tornado Cash smart contracts and cannot blacklist anyone. Should PepperSec become subject to the BSA Regulations or applicable state law though, the process of registration and/or licensure would include the need to register with applicable agencies, maintain appropriate AML, CFT, and/or consumer protection processes, hire and train appropriate staff to satisfy compliance obligations, and observe certain disclosure, reporting, and record retention requirements.

To discuss this Analysis, the requirements and obligations of operating as an MSB, or any related questions, please feel free to reach out directly.